



Haryana Government Gazette

EXTRAORDINARY

Published by Authority

© Govt. of Haryana

No. 170-2017/Ext.] CHANDIGARH, MONDAY, SEPTEMBER 25, 2017 (ASVINA 2, 1939 SAKA)

HARYANA GOVERNMENT
ELECTRONICS & INFORMATION TECHNOLOGY DEPARTMENT
SECRETARIAT FOR INFORMATION TECHNOLOGY

Notification

The 25th September, 2017

No. Admn/315/ISIT/5592.— In view of National Information Security Policy issued by the Department of Home Affairs, Government of India, the Governor of Haryana is pleased to constitute an Information Security Steering Committee (ISSC) under the Chairmanship of Administrative Secretary to Government Haryana, Electronics & Information Technology, Haryana for the State.

2. The composition of the Committee shall be as under:-

- | | |
|--|------------------|
| 1. Administrative Secretary, Electronics & Information Technology | Chairman |
| 2. Secretary/Special Secretary/Jt. Secretary, IT
(as case may be) | Member |
| 3. Chief Information Security Officer (CISO) | Member |
| 4. Finance Advisor | Member |
| 5. Representative of NCIIPC | Member |
| 6. State Informatics Officer, NIC-HSU | Special Invitee. |
| 7. Head SeMT | Special Invitee. |
| 8. Representative of CERT-In | Special Invitee. |

Note: The committee, with the permission of the Chairman may co-opt. or invite such other person(s) as it deemed appropriate to participate in any meeting as special invitee(s).

3. Roles and Responsibilities of the Committee:-

1. **Network change management:** Significant changes to network configuration must be approved by the ISSC.
2. **Application change control:** Each significant change in application must be approved by the ISSC.
3. **Communication of incidents:** The organization must ensure that timely communication is done to report the specific incidents to relevant stakeholders such as the Information Security Steering Committee (ISSC), Sectorial CERT teams and CERT – In-etc. (NCIIPC for CII) .
4. **Management reporting and actions:** Personnel associated with security audit should analyse auditing results to reflect current security status, severity level of the vulnerabilities or anomalies present after removing false- positive and report it to the concerned departments of the organization for remediation. The results of all security audits must be shared with ISSC and senior management.

Chandigarh:
The 30th August, 2017.

DEVENDER SINGH,
Principal Secretary to Government Haryana,
Electronics & Information Technology Department.